IN THE CLAIMS:

Amended claims follow.

1. (Currently Amended) A method for reducing bandwidth needed to transmit key update information for a plurality of members forming a group, comprising:

(a) associating a subgroup of said group with a leaf node of a hierarchical tree, said leaf node having associated therewith a leaf key common to members of said subgroup, wherein upon eviction of at least one member of said group, said leaf key enables said members of said subgroup to receive an update message for an interior node above said leaf node;

wherein said subgroup is a self-repairing group, said self-repairing group being operative to update said leaf key independently;

wherein each of said members of said subgroup is capable of independently updating a shared interior node key.

2. (Original) The method of claim 1, wherein said evicted member is not a part of said subgroup.

3. (Original) The method of claim 1, wherein said evicted member is part of said subgroup.

4. (Cancelled)

5. (Currently Amended) The method of claim 41, wherein said self-repairing group uses a reusable power set.

6. (Original) The method of claim 1, wherein key updates are performed using a logical key hierarchy method.

7. (Original) The method of claim 1, wherein key updates are performed using a one-way function tree method.

8. (Original) The method of claim 1, wherein key updates are performed using a one-way function chain method.

9. (Original) The method of claim 1, wherein said hierarchical tree is a binary tree.

10. (Cancelled)

11. (Currently Amended) A key distribution method, comprising:

(a) evicting at least one member of a group, said group having a plurality of members that share a common node key;

(b) notifying a plurality of members of said group that said at least one member has been evicted; and

(c) determining a new value for said common node key, wherein said determination is capable of being performed independently by said plurality of members of said group;

wherein said plurality of members of said group and said at least one evicted member form a self-repairing group;

wherein each of said members of said group is capable of independently updating the common node key.

12. (Original) The method of claim 11, wherein said evicting comprises evicting one member of said group.

13. (Original) The method of claim 11, wherein said evicting comprises evicting more than one member of said group.

14. (Original) The method of claim 11, wherein said notifying comprises transmitting identities of said at least one evicted member.

15. (Cancelled)

16. (Original) The method of claim 1~~5~~1, wherein said self-repairing group is based on a reusable power set.

17. (Currently Amended) A key distribution method, comprising:

(a) grouping a plurality of said members of said group to form a subgroup of said group, said subgroup having a common key known only to said members of said subgroup, said common key being associated with a common node in a hierarchical tree, said subgroup members being operative to independently update said common key upon eviction of one or more members of said subgroup; and

(b) distributing key update messages for said hierarchical tree upon eviction of one or more members of said subgroup, wherein said distributed key update messages do not update keys associated with nodes below said common node;

wherein said subgroup is self-repairing, and each of said members of said subgroup is capable of independently updating the common key.

18. (Original) The method of claim 17, wherein said subgroup is based on a reusable power set.

19. (Original) The method of claim 17, wherein said key update messages are based on a logical key hierarchy method.

20. (Original) The method of claim 17, wherein said key update messages are based on a one-way function tree method.

21. (Original) The method of claim 17, wherein said key update messages are based on a one-way function chain method.

22. (Original) The method of claim 17, wherein said hierarchical tree is a binary tree.

23. (Cancelled)

24. (Currently Amended) A secret sharing system, comprising:
a key server that is operative to associate a subgroup of a group having a plurality of members with a leaf node of a hierarchical tree, said leaf node having associated therewith a leaf key common to members of said subgroup, wherein upon eviction of at least one member of said group, said key server uses said leaf key to transmit an update message to said members of said subgroup for a key associated with an interior node above said leaf node;
wherein said subgroup is self-repairing, and each of said members of said subgroup is capable of independently updating a shared interior node key.

25. (Currently Amended) A computer program product, comprising:
computer-readable program code for causing a computer to associate a subgroup of a group having a plurality of members with a leaf node of a hierarchical tree, said leaf node having associated therewith a leaf key common to members of said subgroup, wherein upon eviction of at least one member of said group, said leaf key enables said members of said subgroup to receive an update message for a key associated with an interior node above said leaf node; and

a computer-usable medium configured to store the computer-readable program codes;

wherein said subgroup is self-repairing, and each of said members of said subgroup is capable of independently updating a shared interior node key.

26. (New) The method of claim 1, wherein said updating of said shared interior node key is carried out in a single step.

27. (New) The method of claim 1, wherein said updating of said shared interior node key is not dependent on key distribution messages from a root node that update further node keys descending from said shared interior node key.

28. (New) The method of claim 5, wherein said reusable power set uses a power set of said members in said subgroup as a basis for group key updates.

29. (New) The method of claim 28, wherein said reusable power set includes 2^N sets, where N includes the number of said members.

30. (New) The method of claim 28, wherein said reusable power set includes $2^N - 1$ sets, where N includes the number of said members.